

## **Anfrage**

der Abgeordneten Süleyman Zorba, Freundinnen und Freunde

an den Bundesminister für Inneres

betreffend Beschaffung und Einsatz der OSINT-Software „Tangles“ und des Zusatzmoduls „Webloc“

### **BEGRÜNDUNG**

Am 10. Jänner 2025 wurde über die europäische Plattform <https://ted.europa.eu/en/> bekannt gegeben, dass das Bundesministerium für Inneres am 17. Dezember 2024 einen Vertrag über die Beschaffung einer „OSINT Softwarelösung für die österreichischen Ermittlungsbehörden“ im Wert von 847.000 EUR abgeschlossen hat. In der Bekanntmachung wird das beschaffte Produkt näher als OSINT-Software-Lösung „Tangles“ mit „10 Lizenzen + Admin-User“ spezifiziert.

#### **Das Produkt „Tangles“ und der Hersteller Penlink/Cobwebs**

Bei „Tangles“ handelt es sich um ein Analyse- und Überwachungstool, das hauptsächlich für die Auswertung öffentlich zugänglicher Informationen aus dem Web, Social Media und dem Dark Web konzipiert ist und als „Web Intelligence“ oder „Web Investigation Platform“ vermarktet wird. Es wurde ursprünglich durch die Firma Cobwebs hergestellt. Cobwebs wurde 2023 durch PenLinks aufgekauft.

#### **Problematische Aspekte von Tangles**

Die Beschaffung dieser Software wirft mehrere grundsätzliche Bedenken auf.

**Meta/Facebook-Bann wegen missbräuchlicher Aktivitäten:** Im Dezember 2021 veröffentlichte Meta einen Bericht über Bedrohungen durch die „Surveillance-for-Hire Industry“, in dem Cobwebs als bösartiger Anbieter gebrandmarkt und von der Plattform verbannt wurde. Meta entfernte rund 200 Accounts, die von Cobwebs und seinen Kunden weltweit betrieben wurden. Laut dem Bericht betrieben die von Cobwebs-Kunden genutzten Accounts nicht nur Informationssammlung, sondern auch Social Engineering, um geschlossene Communities und Foren zu infiltrieren und Menschen zur Preisgabe persönlicher Informationen zu verleiten. Die Untersuchung identifizierte Kunden in Bangladesch, Hongkong, den USA, Neuseeland, Mexiko, Saudi-Arabien, Polen und anderen Ländern. Neben strafverfolgingsrelevanten Aktivitäten wurde auch häufiges Targeting von Aktivist:innen, Oppositionspolitiker:innen und Regierungsbeamt:innen in Hongkong und Mexiko beobachtet.

## **Das Zusatzmodul „Webloc“ und ADINT-Technologien**

Von besonderer Brisanz ist das Zusatzmodul „Webloc“ für Tangles. Webloc ermöglicht den Zugriff auf kommerzielle Standortdaten und Web-/App-Verhaltensdaten, die aus der digitalen Werbeindustrie, von Datenhandelsfirmen oder direkt von Website- und App-Anbietern stammen. Diese Praxis wird unter dem Begriff „Advertising Intelligence“ (ADINT) zusammengefasst und beschreibt die Nutzung von Daten aus Smartphone-Apps und digitaler Werbung für Überwachungszwecke.

Die Hersteller halten sich über ihre Anwendung Webloc sehr bedeckt. Eine archivierte Produktseite auf der Cobwebs-Website aus dem Jahr 2021 beschrieb Webloc als „Location Intelligence System“, wurde jedoch kurz nach ersten kritischen Medienberichten offline genommen. Die aktuelle Penlink-Website erwähnt lediglich einen Trainingskurs für Webloc.

Aus öffentlich zugänglichen Beschaffungsunterlagen von US-Behörden geht hervor, dass Webloc folgende Daten für Überwachungszwecke zur Verfügung stellt:

GPS-Standortdaten von mobilen Apps

Genutzte Apps

Geschlecht, Alter, Sprachen

Interessen

Gerätetyp

Mobile Geräte-IDs (Advertising IDs)

Webloc wird bereits von zahlreichen US-Behörden eingesetzt, von kleinen lokalen Polizeidienststellen und Sheriffs bis hin zum Department of Homeland Security und der Einwanderungs- und Zollbehörde ICE.

## **Datenschutzrechtliche Bedenken**

Die mobile Geräte-IDs (insbesondere IDFA bei iOS und AAID bei Android) werden in der digitalen Werbewelt flächendeckend für Profiling-Zwecke verwendet. Von diesen IDs kann leicht auf die Personen geschlossen werden, die die Geräte nutzen. Die Daten gelangen von Websites und Apps entweder über das digitale Werbesystem Real-Time Bidding (RTB) oder über in die Websites/Apps eingebaute Drittanbieter-Tracking-Pixel und -Software zu Datenhandelsfirmen, die sie direkt oder indirekt an Firmen wie Cobwebs/Penlink verkaufen.

Diese gesamte Datenlieferkette ist datenschutzrechtlich höchst problematisch. Die zweckwidrige Verarbeitung von Standort- und Verhaltensdaten von Smartphone-Apps und aus der digitalen Werbung für die Überwachung durch staatliche Behörden ist nach Ansicht von Datenschutzexpert:innen rechtswidrig – entlang der gesamten Datenlieferkette bis hin zur Verarbeitung durch Cobwebs/Penlink. Die betroffenen Personen haben in der Regel keine Kenntnis von derartigen Verarbeitungen und haben sicherlich nicht wirksam in eine solch weitreichende Datenverarbeitung eingewilligt.

In mehreren US-Bundesstaaten und auf EU-Ebene wird die Verwendung solcher kommerzieller Überwachungsdaten durch Strafverfolgungsbehörden zunehmend kri-

tisch diskutiert. Expert:innen warnen, dass durch den Ankauf kommerzieller Daten Behörden rechtliche Schranken umgehen, die bei der direkten Erhebung solcher Daten greifen würden.

### **Transparenz und demokratische Kontrolle**

Angesichts der beschriebenen grundrechtlichen Implikationen, der fragwürdigen Geschäftspraktiken des Anbieters und der datenschutzrechtlichen Bedenken ist es von höchstem öffentlichem Interesse, umfassende Transparenz über die Beschaffung und den geplanten Einsatz dieser Überwachungstechnologie herzustellen. Insbesondere muss ausgeschlossen werden, dass über das Zusatzmodul Webloc oder vergleichbare ADINT-Technologien kommerzielle Standort- und Verhaltensdaten aus der digitalen Werbeindustrie für polizeiliche Ermittlungen in Österreich eingesetzt werden.

Die unterfertigenden Abgeordneten stellen daher folgende

## **ANFRAGE**

### **A) Beschaffung und Umfang der Software „Tangles“**

- 1) Wann wurde die Entscheidung zur Beschaffung von „Tangles“ getroffen und wer war in diese Entscheidung eingebunden?
- 2) Welche alternativen OSINT-Softwarelösungen wurden im Vorfeld der Beschaffung evaluiert?
  - a. Nach welchen Kriterien erfolgte die Auswahl von Tangles?
  - b. Gab es eine öffentliche Ausschreibung oder ein beschränktes Vergabeverfahren?
- 3) Wie setzen sich die Gesamtkosten von 847.000 EUR konkret zusammen?
  - a. Welcher Anteil entfällt auf Lizenzgebühren?
  - b. Welcher Anteil entfällt auf Implementierung und Schulung?
  - c. Welcher Anteil entfällt auf Wartung und Support?
  - d. Für welchen Zeitraum gilt der Vertrag?
- 4) Welche Module und Funktionen von Tangles wurden konkret beschafft?
  - a. Bitte um eine detaillierte Auflistung aller im Vertrag enthaltenen Module und Zusatzfunktionen.

- b. Welche Datenquellen kann die beschaffte Software-Konfiguration auswerten?
- 5) Welche organisatorischen Einheiten des BMI oder nachgeordneter Behörden werden Tangles nutzen?
- a. Wie viele Personen werden insgesamt Zugang zu Tangles haben?
  - b. Für welche konkreten Einsatzbereiche und Ermittlungsarten ist die Nutzung vorgesehen?

## **B) Das Zusatzmodul „Webloc“ und kommerzielle Standortdaten**

- 6) Wurde das Tangles-Zusatzmodul „Webloc“ beschafft?
- a. Wenn ja, seit wann ist es im Einsatz und zu welchen Kosten?
  - b. Wenn ja, welche Datenquellen werden über Webloc zugänglich gemacht?
  - c. Wenn nein, wurde Webloc als Demo-Version oder Trial-Version getestet?
- 7) Gab es Angebote, Gespräche, Verhandlungen, Schulungen oder Anfragen bezüglich des Zusatzmoduls „Webloc“?
- a. Wenn ja, wann fanden diese statt und mit welchem Ergebnis?
  - b. Wenn ja, welche Funktionalitäten und Datenquellen wurden dabei vorgestellt oder angeboten?
  - c. Hat Penlink/Cobwebs proaktiv das Modul Webloc angeboten oder beworben?
- 8) Plant das BMI die Beschaffung oder Nutzung von Webloc in der Zukunft?
- 9) Nutzen das BMI oder nachgeordnete Behörden kommerzielle Standortdaten von Smartphone-Apps für Ermittlungszwecke?
- a. Wenn ja, über welche Software-Lösungen oder Dienstleister erfolgt der Zugriff?
  - b. Wenn ja, seit wann werden solche Daten genutzt?
  - c. Wenn ja, auf welcher Rechtsgrundlage erfolgt die Nutzung?
  - d. Wenn nein, ist eine solche Nutzung in Zukunft geplant?

### C) ADINT-Technologien und alternative Anbieter

10) Gibt es Verträge, Korrespondenzen oder Unterlagen des BMI oder nachgeordneter Behörden aus den letzten drei Jahren, die sich auf „ADINT“, „Ad Intelligence“, „Advertising Intelligence“ oder „Advertisement Intelligence“ beziehen?

11) Wurden folgende alternative OSINT- oder ADINT-Software-Lösungen und deren Anbieter evaluiert, getestet oder beschafft:

- a. Babel Street (Produkt „Locate X“)
- b. Rayzone Group (Produkt „Echo“)
- c. Insanet (Produkt „Sherlock“)
- d. Intelos (Produkt „Adhoc“)
- e. Shadowdragon (Produkt „Horizon Investigate“)
- f. Bsightful
- g. Patternz
- h. S2T
- i. Octostar
- j. Siren
- k. RCS Labs
- l. GeoGence
- m. Intellexa (Produkt „Aladdin“)

12) Plant das BMI die Beschaffung weiterer OSINT- oder ADINT-Technologien?

- a. Wenn ja, welche Produkte oder Anbieter werden in Betracht gezogen?
- b. Wenn ja, welches Budget ist dafür vorgesehen?

### D) Datenschutzrechtliche Prüfung

13) Wurde vor der Beschaffung von Tangles eine datenschutzrechtliche Folgenabschätzung gemäß Art. 35 DSGVO durchgeführt?

- a. Wenn ja, mit welchem Ergebnis?
- b. Wenn ja, wurde die Datenschutzbehörde gemäß Art. 36 DSGVO konsultiert?
- c. Wenn nein, warum nicht?

14) Wurde geprüft, ob die von Tangles zugänglich gemachten Daten rechtmäßig erhoben und verarbeitet wurden?

- a. Wenn ja, wie erfolgte diese Prüfung und mit welchem Ergebnis?

- b. Wie wird sichergestellt, dass nur rechtmäßig erhobene Daten verwendet werden?

15) Welche Vorkehrungen wurden getroffen, um sicherzustellen, dass über Tangles keine Daten verarbeitet werden, die entlang der Lieferkette unter Verstoß gegen die DSGVO erhoben wurden?

16) Wurden rechtliche Bedenken hinsichtlich der Nutzung kommerzieller Daten aus der digitalen Werbeindustrie für polizeiliche Ermittlungen erörtert?

- a. Wenn ja, mit welchem Ergebnis?
- b. Welche Rechtsabteilungen oder externen Gutachter waren eingebunden?

#### **E) Sicherheitsüberprüfung des Anbieters**

17) Wurde vor der Beschaffung eine Sicherheitsüberprüfung des Anbieters Penlink/Cobwebs durchgeführt?

- a. Wenn ja, durch wen und mit welchem Ergebnis?
- b. Wenn ja, wurden dabei die Verbindungen zu anderen Überwachungstechnologie-Anbietern geprüft?
- c. Wenn nein, warum nicht?

18) War dem BMI bei Vertragsabschluss bekannt, dass Meta/Facebook im Jahr 2021 etwa 200 Accounts von Cobwebs und dessen Kunden wegen missbräuchlicher Aktivitäten und Social Engineering entfernt hat?

- a. Wenn ja, wie wurde diese Information bewertet?
- b. Wenn nein, wie wird diese Information nachträglich bewertet?

19) Wurden die Eigentümerstrukturen und Geschäftsverbindungen von Penlink/Cobwebs überprüft?

- a. Wenn ja, mit welchem Ergebnis?

#### **F) Technische Spezifikationen und Datenschutz**

20) Welche technischen und organisatorischen Maßnahmen wurden implementiert, um den Missbrauch von Tangles zu verhindern?

21) Wie wird protokolliert und kontrolliert, welche Personen welche Daten über Tangles abfragen?

- a. Wer hat Zugriff auf diese Protokolle?

b. Wie lange werden diese Protokolle aufbewahrt?

22) Gibt es Beschränkungen, welche Datenquellen über Tangles abgefragt werden dürfen?

a. Wenn ja, wie lauten diese Beschränkungen?

b. Wie werden diese Beschränkungen technisch durchgesetzt?

23) Hat das BMI Zugriff auf den Quellcode von Tangles oder erfolgte eine unabhängige Sicherheitsüberprüfung der Software?

a. Wenn ja, durch wen und mit welchem Ergebnis?

b. Wenn nein, wie wird sichergestellt, dass die Software keine unerwünschten Funktionen oder Sicherheitslücken enthält?

### **G) Rechtsgrundlagen und Einsatzszenarien**

24) Auf welcher Rechtsgrundlage erfolgt der Einsatz von Tangles?

25) Für welche konkreten Deliktsbereiche ist der Einsatz von Tangles vorgesehen?

a. Gibt es Einschränkungen hinsichtlich der Schwere der zu ermittelnden Straftaten?

b. Ist der Einsatz auch zur Gefahrenabwehr vorgesehen?

26) Ist der Einsatz von Tangles zur Überwachung von Versammlungen oder Demonstrationen vorgesehen?

a. Wenn ja, unter welchen Voraussetzungen?

b. Wenn nein, wie wird ein solcher Einsatz ausgeschlossen?

27) Welche internen Richtlinien oder Dienstanweisungen regeln den Einsatz von Tangles?

a. Bitte um Übermittlung dieser Dokumente.

### **H) Erfahrungen anderer Länder und internationale Zusammenarbeit**

28) Wurden vor der Beschaffung Erfahrungen anderer EU-Mitgliedstaaten mit Tangles oder vergleichbaren OSINT-Tools eingeholt?

a. Wenn ja, von welchen Ländern und mit welchen Erkenntnissen?

29) Wurden Erfahrungen von Ländern außerhalb der EU eingeholt?

a. Wenn ja, von welchen Ländern?

b. Wurden dabei auch kritische Berichte über den Einsatz gegen Demonstrant:innen oder Journalist:innen berücksichtigt?

30) Gibt es eine internationale Zusammenarbeit mit anderen Strafverfolgungsbehörden über Tangles?

a. Wenn ja, mit welchen Ländern und in welcher Form?

b. Werden dabei Daten ausgetauscht?

#### **I) Transparenz und parlamentarische Kontrolle**

31) Wie viele Ermittlungsverfahren wurden seit Inbetriebnahme von Tangles unter Nutzung dieser Software geführt?

a. In wie vielen Fällen führte die Nutzung von Tangles zu verwertbaren Erkenntnissen?

b. In wie vielen Fällen wurden Personen aufgrund von über Tangles gewonnenen Erkenntnissen angeklagt?

32) Wird der ständige Unterausschuss des Ausschusses für innere Angelegenheiten regelmäßig über den Einsatz von Tangles informiert?

a. Wenn ja, in welchen Abständen und in welcher Form?

b. Wenn nein, ist eine solche regelmäßige Information geplant?

33) Ist geplant, die Öffentlichkeit über den Einsatz von Tangles zu informieren?

a. Wenn ja, in welcher Form und in welchem Umfang?

b. Wenn nein, warum nicht?

34) Wie wird die Einhaltung der datenschutzrechtlichen Vorgaben bei der Nutzung von Tangles kontrolliert?

a. Ist die Datenschutzbehörde in die Kontrolle eingebunden?

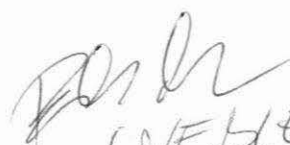
b. Gibt es regelmäßige Audits?

  
(SCHWAB)

  
(SCHALLER) (SCHALLER)

  
(SCHWAB)

  
(LADIC)

  
(NEHLER)

